Beitrag 11

Rollenmanagement und Rechteverwaltung

Alexander Lawall
Professur für Produktionswirtschaft und Informationstechnik
alexander.lawall@iisys.de

Abstract: Das Thema besteht aus zwei Hauptteilen, der Entwicklung eines Metamodells zur Abbildung der Aufbauorganisation und einer deklarativen Sprache für die Definition der Rechte und Pflichten in Unternehmen.

Das Metamodell beinhaltet die Primär- und Sekundärorganisation, domänenspezifische Relationen (z.B. Vorgesetzten-, Berichts- und Stellvertreterbeziehungen) und Attribute für die Strukturelemente. Betriebliche Aufgabenträger können mit ihren Relationen im Organisationsmodell, konsistent zum Metamodell, abgebildet werden.

Als zweiter Aspekt wird eine deklarative Sprache entwickelt. Die Sprache wird für die Zuweisung von Aufgaben zu Aufgabenträgern und die Definition von Zugriffsrechten eingesetzt. Sie wird als Anfragesprache von Anwendungssystemen an den logisch zentralen Organisationsserver (enthält das Organisationsmodell) und die Formulierung von Prädikaten (Sprachausdrücke auf Relationen) verwendet.

Einleitung, Problemstellung und Einordnung

Untersucht man betriebliche Anwendungssysteme (AwS), fällt auf, dass in vielen Applikationen *redundant* Informationen über die Organisationsstruktur mit ihren Beteiligten und den jeweiligen (Zugriffs-)Rechten und Pflichten verwaltet werden. Einerseits führt dies zu einem hohen Pflegeaufwand auf der Administratorenseite, andererseits müssen sich die Benutzer eine Vielzahl von Benutzerkennungen merken. Um diese Situation zu verbessern, wurden Verfahren wie das „Single-Sign-On" entwickelt, die auf Basis eines zentralen Verzeichnisdienstes, wie dem Active Directory von Microsoft, die Systemanmeldung eines Benutzers an das genutzte AwS weiterreichen. Der Mitarbeiter muss sich somit nicht gegenüber mehreren Applikationen authentifizieren, was zunächst einen Vorteil bringt. Die Authentifizierung ist allerdings nur eine Seite der Medaille. Es bleibt das Problem bestehen, dass jedes AwS eigene technologische Verfahren vorhält, um Zugriffsrechte zu verwalten oder – im Falle von Workflow-Systemen – Aufgaben zuzuweisen (siehe Abbildung 16.1). Der Neuzugang, die Versetzung oder das Ausscheiden eines Mitarbeiters zieht somit einen hohen Administrationsaufwand in allen eingesetzten Systemen nach sich und ist fehleranfällig.

Es ist nun eine Innovation, ein Metamodell für die Aufbauorganisation eines Unternehmens zu formalisieren und konsistente Organisationsmodelle zu instantiieren. Beliebige Anwendungssysteme, wie zum Beispiel Datenbank-Management-, ERP-, Workflow-Management- oder Portal-Systeme können sich dieses Modell nutzbar machen. Bei diesem Verfahren werden Zugriffsrechte und Verantwortungen mittels einer deklarativen Sprache formuliert, die an Hand des Organisationsmodells interpretiert wird und deren Ausdrücke zentralisiert ausgewertet werden (siehe Abbildung 16.2). Die Umsetzung eines konsistenten Rechtesystems vereinfacht sich dadurch stark.

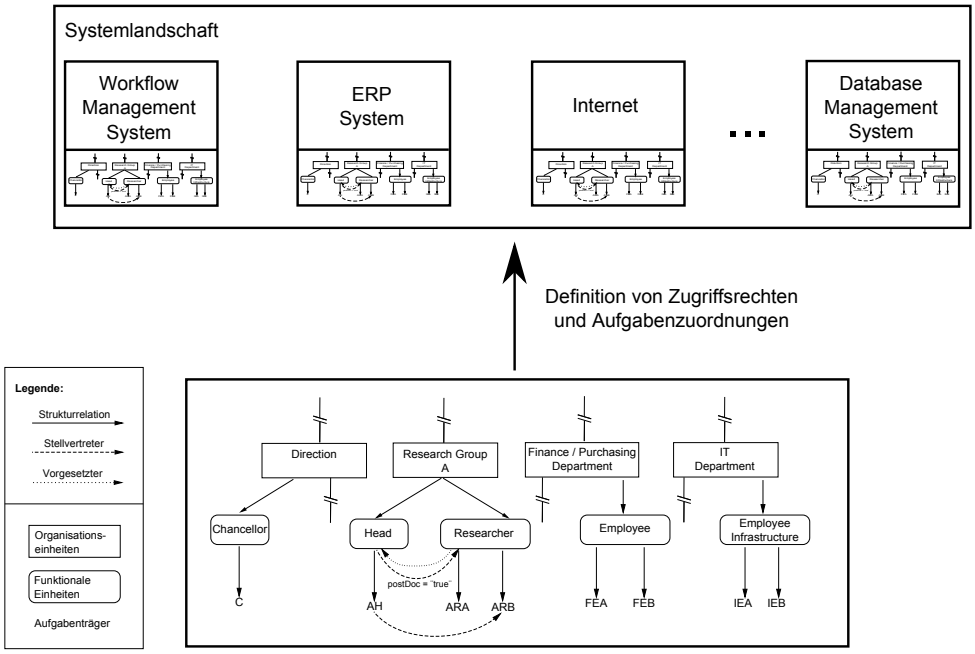

Abbildung 16.1: Redundanz in betrieblichen Anwendungssystemen

Stand der Wissenschaft und Technik

Die verschiedenen Anforderungen für eine Metamodell resultieren aus der Organisationstheorie (speziell Aufbauorganisation), der Abbildung von organisatorischen Entitäten und den Relationen zwischen diesen. Die Definition von aufbauorganisatorischen Zusammenhängen der Primär- und Sekundärorganisation, wie Einlinien-, Mehrlinien- und Stablinienorganisation legt das Fundament für ein Metamodell für Unternehmensstrukturen (vgl. [Vah07]). Neben den klassischen Organisationsformen

(wie hierarchische Organisation, Matrix- bzw. Tensororganisation, Netzwerkorganisation, Teamorganisation u.v.m.) gibt es neben den intra- ebenso inter-organisatorische Modellanforderungen. Supply Chain Management und die verteilte Produktentwicklung sind zwei Formen davon.

Für die Definition von Rechten und Aufgaben existieren die Konzepte *Role-based Access Control* (RBAC)[1] und Attribute-based Access Control (ABAC)[2]. Auch weitere Ansätze, wie *Mandatory Access Control* (MAC) und *Discretionary Access Control*, berücksichtigen das Problem des aufbauorganisatorischen Kontext jedoch nicht ausreichend. Die Technologien der Identity- und Access-Management-Systeme unterscheiden sich sowohl in den Konzepten als auch in der systemspezifischen Implementierung.

Die genannten Konzepte bilden die Basis für zahlreiche Systeme, unter anderem Verzeichnisdienste, Identity und Access Management oder Enterprise Resource Planning (ERP) Lösungen. *Lightweight Directory Access Protocol* (LDAP) bildet hierarchisch Daten ab. Die Attribut/Wert-Paare werden genutzt, um organisatorischen Kontext zu strukturieren und Benutzerdaten zu verwalten. Das Microsoft Active Directory enthält ein spezifisches Schema von LDAP als Komponente. Die ermöglicht Relationen, die über hierarchische Organisationsstrukturen hinausgehen, zu modellieren (z.B. Mitglied einer Gruppe). Axiomatics ist ein Produkt, das den attributbasierten Ansatz realisiert. Rechte werden an Eigenschaften von Subjekten (z.B. Aufgabenträger) und den Objekten (z.B. Datei), auf denen eine Aktion ausgeführt wird, zugewiesen. Im Kontrast dazu ist SAP NetWeaver Identity Management ein Modul, das die Zuweisung von Rollen zu Subjekten verantwortlich ist. Komplexere Sachverhalte, wie Relationen zwischen Rollen sind nicht möglich.

Für das Forschungsvorhaben lassen sich folgende Forschungsfragen formulieren:

1. *Welche Komponenten beinhaltet ein aufbauorganisatorisches (Meta-)Modell?*
2. *Wie lassen sich (Zugriffs-)Rechte und Aufgaben deklarativ mit einer Sprache abbilden?*
3. *Inwiefern lässt sich die Laufzeit für die Interpretation einer Anfrage auf dem Organisationsmodell mit graphentheoretischen Ansätzen verbessern?*

Die Methodik folgt dem konstruktionsorientierten Forschungsansatz. Es werden Anforderungen analysiert, ein (Meta-)Modell gebildet, ein Prototyp implementiert und dieser gegen die Anforderungen validiert. Anforderungen sind die Definition von En-

[1] Die Definition von Rechten und Aufgabenzuweisungen basierend auf Rollen, siehe [WS+09, S. 89].

[2] Verwendung von Attributen zur Rechte- und Aufgabenzuweisung, beschrieben in [KCW10].

titäten, wie Organisationseinheiten (z.B. Abteilung und Unterabteilung), funktionalen Einheiten (z.B. Manager und Sachbearbeiter) und personellen und maschinellen Aufgabenträgern (vgl. das Organisationsmodell der Abbildung 16.1). Verschiedene Relationen verbinden diese Entitäten strukturell bzw. domänenspezifisch, beschrieben in [LRS11]. Weitere Anforderungen an das Metamodell und die deklarative Sprache sind in [LSR12], [LSR13a] und [LSR13b] aufgeführt.

Forschungsziel und Schluss

Das Ziel ist die Einbettung des Metamodells, des resultierenden Organisationsmodells und des Interpreters der deklarativen Sprachausdrücke in einen Organisationsserver, siehe Abbildung 16.2. Die angebundenen Anwendungssysteme stellen dann Anfragen – formuliert über die Sprache – an den Organisationsserver. Nach der Interpretation des Ausdrucks am Organisationsmodell wird das Ergebnis (z.B. Menge an Aufgabenträgern) an das fragende Anwendungssystem zurück gesendet. Die Sprachausdrücke sind in den Anwendungssystemen in unterschiedlichen Ausprägungen im Einsatz. Eine Objekt-/Zugriffsmatrix für Dateien, eine Zuordnung einer Aufgabe eines Workflows zu Aufgabenträgern oder die Formulierung von Zugriffsrechten für Tabellen einer Datenbank sind einige Beispiele dafür.

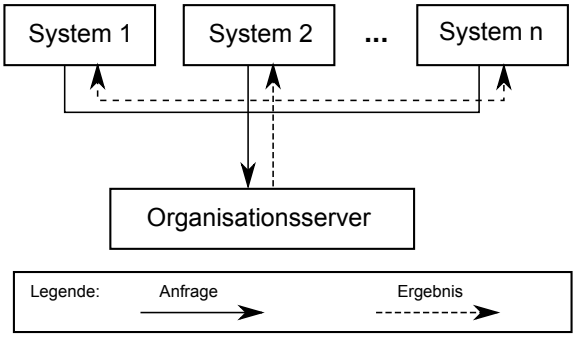

Abbildung 16.2: Einbettung des Organisationsserver in die Systemlandschaft.

Literaturverzeichnis

[KCW10] Kuhn, D R; Coyne, E J; Weil; T R. Adding Attributes to Role-Based Access Control. *Computer*, 43(6):79–81, 2010.

[LRS11] Lawall, A; Reichelt, D; Schaller, T. Intelligente Verzeichnisdienste. In Barton, T; Erdlenbruch, B; Herrmann, F; Müller, C; (Hrsg.) *Herausforderungen an die Wirtschaftsinformatik: Betriebliche Anwendungssysteme*, AKWI 2011, S. 87–100, News & Media, Berlin, 2011.

[LSR12] Lawall, A; Schaller, T; Reichelt, D. An Approach towards Subject-Oriented Access Control. In *S-BPM ONE 2012*, S. 33–42, Springer-Verlag, Heidelberg, 2012.

[LSR13a] Lawall, A; Schaller, T; Reichelt, D. Integration of Dynamic Role Resolution within the S-BPM Approach. In *S-BPM ONE 2013*, S. 21–33, Springer-Verlag, Heidelberg, 2013.

[LSR13b] Lawall, A; Schaller, T; Reichelt, D. Who Does What – Comparison of Approaches for the Definition of Agents in Workflows. In *Web Intelligence (WI) and Intelligent Agent Technologies (IAT), 2013 IEEE/WIC/ACM International Joint Conferences on*, S. 74–77, Nov 2013.

[Vah07] Vahs, D. *Organisation: Einführung in die Organisationstheorie und -praxis*. Schäffer-Poeschel, 2007.

[WS+09] Williamson, G; Sharoni, I; Yip, D; Spaulding, K. In *Identity Management: A Primer*, Mc Press Series, MC Press Online, 2009.

Alexander Lawall, M. Eng., absolvierte an der Hochschule für Angewandte Wissenschaften Hof die Studien Technische Informatik und den postgraduierten Master Software Engineering for Industrial Applications. Der Anstellung an der Universität Bayreuth folgend, arbeitet er bis heute als wissenschaftlicher Mitarbeiter am Institut für Informationssysteme (IISYS) in der Arbeitsgruppe Informationsmanagement und ist des Weiteren in der Lehre tätig.

Dieser Beitrag ist erschienen in: Thorsten Claus und Niels Seidel (Hrsg.), *Werkstatt europäischen Denkens – 20 Jahre Internationales Hochschulinstitut Zittau*, TUDpress, Dresden, 2014. Online verfügbar: http://nbn-resolving.de/urn:nbn:de:bsz:14-qucosa-152320.